Legacy Systems

Description

Describes the kinds of security risks that can be present in legacy systems, both in-house and commercial off-the-shelf (COTS), and offers guidance for assessing those risks and making sound decisions about addressing them.

Overview Articles

Name	Version Creation Time	Abstract
Software Security in Legacy Systems	2/22/07 3:30:21 PM	Much of the emphasis in your organization is undoubtedly on new systems work. You certainly have well-developed processes for building new systems, and you carefully track new software development activity. This attention is appropriate, since it is not simple to install new software, test it fully, and deploy it throughout the organization. Typically, though, a large portion of your code base lies in the legacy systems. Not just the major systems, but a myriad of smaller systems in every corner of the organization. These legacy systems do the hard, day-to-day work of your organization. Further, a considerable portion of your systems development work is directed at maintenance and extension of these existing systems, though these smaller projects are often done without benefit of the rigorous methods, independent review, and management attention devoted to new systems work. The result is increased performance risk and greater security risk.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Assessing Security Risk In	4/20/07 1:27:59 PM	This article outlines a general

Legacy Systems		approach to assessing the security risk posed by your existing business systems#the systems already in place within your organization. This approach has four steps: identifying and describing the legacy systems, selecting the legacy systems that are most likely to present a risk, quickly evaluating the risks that each “most likely” system poses to the enterprise, and finally developing a strategy to mitigate risk, reducing it to an acceptable level.
Software Security in Legacy Systems	2/22/07 3:30:21 PM	Much of the emphasis in your organization is undoubtedly on new systems work. You certainly have well-developed processes for building new systems, and you carefully track new software development activity. This attention is appropriate, since it is not simple to install new software, test it fully, and deploy it throughout the organization. Typically, though, a large portion of your code base lies in the legacy systems. Not just the major systems, but a myriad of smaller systems in every corner of the organization. These legacy systems do the hard, day-to-day work of your organization. Further, a considerable portion of your systems development work is directed at maintenance and extension of these existing systems, though these smaller projects are often done without benefit of the rigorous methods, independent review, and management attention devoted to new systems work. The result is increased performance risk and greater security risk.
Security Considerations in Managing COTS Software	1/5/07 5:07:55 PM	Security failures can have severe consequences whether they are rooted in COTS or custom code. This, coupled with the ubiquity and opacity of COTS software,

		makes it a critical and difficult problem that an organization ignores at its own extreme peril, however convenient that is to do.

All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
Assessing Security Risk In Legacy Systems	4/20/07 1:27:59 PM	This article outlines a general approach to assessing the security risk posed by your existing business systems#the systems already in place within your organization. This approach has four steps: identifying and describing the legacy systems, selecting the legacy systems that are most likely to present a risk, quickly evaluating the risks that each “most likely” system poses to the enterprise, and finally developing a strategy to mitigate risk, reducing it to an acceptable level.
Security Considerations in Managing COTS Software	1/5/07 5:07:55 PM	Security failures can have severe consequences whether they are rooted in COTS or custom code. This, coupled with the ubiquity and opacity of COTS software, makes it a critical and difficult problem that an organization ignores at its own extreme peril, however convenient that is to do.
Software Security in Legacy Systems	2/22/07 3:30:21 PM	Much of the emphasis in your organization is undoubtedly on new systems work. You certainly have well-developed processes for building new systems, and you carefully track new software development activity. This attention is appropriate, since it is not simple to install new software, test it fully, and deploy it throughout the organization. Typically, though, a large portion of your code base lies in the legacy systems. Not just the major systems, but a myriad of

		smaller systems in every corner of the organization. These legacy systems do the hard, day-to-day work of your organization. Further, a considerable portion of your systems development work is directed at maintenance and extension of these existing systems, though these smaller projects are often done without benefit of the rigorous methods, independent review, and management attention devoted to new systems work. The result is increased performance risk and greater security risk.

Fields

Name	Value
Categories	best-practices